The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE

Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.

http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
03/24/2016

SUBJECT:
Vulnerability in Oracle Java SE Could Allow for Remote Code Execution

OVERVIEW:
A vulnerability in Oracle Java SE for desktop web browsers could allow for remote code execution. This vulnerability does not affect Java deployments, such as those in servers or standalone applications that run only trusted code nor does it affect Oracle server-based software. Successful exploitation of this vulnerability may allow for remote code execution in the context of the current application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

THREAT INTELLIGENCE
Technical details of the vulnerability have been publicly disclosed. There are no reports that this vulnerability is being used in the wild at this time.

SYSTEMS AFFECTED:
- Oracle Java SE 7 Update 97
- Oracle Java SE 8 Update 73 and 74

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:
Oracle Java SE is vulnerable to a remote code execution vulnerability due to a flaw in its 'Hotspot' sub-component. This vulnerability can be exploited when a user running an unpatched version of Java SE visits a malicious web page.

Successful exploitation of this vulnerability may allow for remote code execution in the context of the current application. Depending on the privileges associated with the application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Install the updates provided by Oracle immediately after appropriate testing.
- Remind users not to visit websites or follow links provided by unknown or untrusted sources.
- Limit application and user access to only what is required.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:
Oracle:
http://www.oracle.com/technetwork/topics/security/alert-cve-2016-0636-2949497.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0636